STATE OF ALABAMA

Information Technology Standard

Standard 660-02S2_Rev A: PDA Security

1. INTRODUCTION:

Personal Digital Assistant (PDA) devices combine mobile computing and networking features in a pocket-sized device. The benefits PDA devices provide: their small size, portability, and their ability to store large amounts of information along with the breadth of communication options available, also expose the organization to many security risks.

2. OBJECTIVE:

Establish implementation requirements for PDA devices connecting to the State of Alabama network.

3. SCOPE:

These requirements apply to PDA devices that are configured to send/receive State of Alabama email or connect to State network applications and/or data and to the system components required to support such devices (including):

- Wireless handheld device (e.g., PDA, Smartphone)
- Software installed on the handheld device by the device manufacturer or wireless carrier (e.g. operating system, internet browser, productivity applications)
- Wireless email product client and server software
- IT Security Policy Management Server
- Gateway Server, located with the IT Security Policy Management Server, providing connection between the wireless handheld device and enterprise network services

Requirements apply to all brands of PDA (including but not limited to Blackberry, Treo, iPhone, and Palm devices).

4. REQUIREMENTS:

4.1 GENERAL REQUIREMENTS

State-owned PDA devices shall be used for official duties only.

Email redirection (push email) from the Exchange Server to the wireless handheld device shall be controlled via a centrally managed server. Desktop or Internet controlled email redirection is not authorized.

4.2 POLICY MANAGEMENT REQUIREMENTS

Centrally manage the following PDA security policies:

4.2.1 User Authentication

Enforce user authentication using a PIN, password, or passphrase to unlock the device.

The PIN/Password policy shall meet the requirements specified in State IT Standard 620-03S1: Authentication-Passwords.

4.2.2 Inactivity Timeout

The handheld device shall utilize an inactivity timeout whereby the user must reenter their user PIN/password to unlock the device. Set the device inactivity timeout setting to no more than 15 minutes.

4.2.3 Data Wipe

The system administrator shall have the capability to remotely transmit a “data wipe” (hard reset) command to the handheld device. The “Data Wipe” function will erase all data (operating system, applications, and data) stored in user addressable memory on the handheld device.

4.2.4 Text Messaging

If the wireless email system provides text messaging service, the service shall be S/MIME (v3 or later) enabled.

The system administrator shall disable the following mobile text messaging services:

- Short Message Service (SMS)
- Multimedia Messaging Service (MMS)

Information sent via available text messaging services should be logged (recommended).

4.3 DEVICE REQUIREMENTS

4.3.1 User Authentication to Unlock Device

The handheld device must be protected by authenticated logon using a PIN, password, or passphrase. A user cannot bypass device authentication.

4.3.2 Hot-sync Operations

Hot-sync management software shall use some form of access control (e.g., user password is entered before a hot-sync operation can be executed)

Wireless operations shall be disabled when a PDA is connected to the State of Alabama wired network via a hot-sync or other interface cable

PDA’s that transmit, receive, store, or process State Sensitive or Confidential information shall not be synced to home or personally owned PCs

4.3.3 Physical Safeguards

Asset tag or engrave the device by permanently marking (or engraving) the outer case or an accessible internal area with the agency name, address, and phone number.

Never leave a PDA device in a vehicle where it can be seen through a window. Also keep in mind that the extreme temperature ranges within a vehicle could easily destroy the PDA, and render the information on the device inaccessible.

4.3.4 Other Security Controls

Where necessary, restrict or prohibit the use of PDA's with digital cameras (still and video) to protect sensitive and confidential information.

Disable peer-to-peer (ad-hoc) networking capabilities, if so equipped, to prevent inadvertent peer-to-peer communications

4.4 PERSONALLY-OWNED DEVICE REQUIREMENTS

Personally-owned PDA's shall not be connected to the State network or systems unless specifically approved in writing by the IT Manager or similar authority.

When connecting to State networks personally-owned PDA's shall comply with the requirements stated in this and other applicable state standards. The written approval to connect a personally-owned PDA to the State network shall include a reference to these requirements as well as stated limitations regarding the level of service provided to non-state-owned devices.

4.4.1 Technical Support

Support for personally-owned PDA devices is the owner's responsibility. State support personnel will perform only limited support such as provisioning the device so it can receive State email and connect to State network resources and limited diagnostic activities to establish whether a problem is hardware, software, or security incident related.

4.4.2 Forfeiture

PDA owners shall sign a forfeiture agreement stating that in the event a personally-owned PDA is involved in a security incident, investigative personnel have the right (and responsibility) to secure and examine the device for forensics purposes. Devices shall be returned to the owner when no longer needed.

4.4.3 Device Sanitization and Disposal

State media sanitization standards require sanitization of PDA devices prior to disposal or reuse. Users of personally-owned PDA devices used to connect to State networks shall also observe these device sanitization and disposal requirements when turning devices in for upgrade, repair or service termination. System Administrators shall ensure devices have been cleared upon changes in employment (transfer, resignation, retirement, termination, etc.).

4.5 LOST DEVICES

User shall immediately report the loss of any PDA (including personally-owned PDA's if used to connect to State networks or store State data) to their manager, IT Manager, or ISO. Administrators shall perform a data wipe command to clear the device memory.

Do not connect a previously lost device to any operational network or system until the device has been properly sanitized (hard reset) and re-provisioned.

4.6 AWARENESS & TRAINING

PDA users shall be provided awareness level training (in accordance with State standards) on the security vulnerabilities presented by use of such devices and on appropriate use.

5. DEFINITIONS:

PERSONAL DIGITAL ASSISTANT (PDA): Includes Personal Electronic Devices (PEDs), email and Smartphone devices such as Blackberry, Treo, and other handheld communication devices that have similar inherent features and vulnerabilities.

PUSH EMAIL: A delivery system with real-time capability to "push" email through to the client device as soon as it arrives, rather than requiring the client to poll and collect or pull mail manually.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 620-02: System Security

6.2 RELATED DOCUMENTS

Information Technology Standard 620-03S1: Authentication - Passwords

Information Technology Standard 680-01S4: Media Sanitization

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	2/20/2008	
Rev A	7/15/2008	Deleted iPhone exception from Scope.